

ABSTRACT

Objects captured over a network by a capture system can be indexed to provide enhanced search and content analysis capabilities. In one embodiment the objects can be indexed using a data structure having a source address field to indicate an origination address of the object, a destination address field to indicate a destination address of the object, a source port field to indicate an origination port of the object, a destination port field to indicate a destination port of the object, a content field to indicate a content type from a plurality of content types identifying a type of content contained in the object, and a time field to indicate when the object was captured. The data structure may also store a cryptographic signature of the object to ensure the object is not altered after capture.